Theoretical Computer Science 43 (1986) 189-200
North-Holland

COMPLETE SETS OF UNIFIERS AND MATCHERS IN EQUATIONAL THEORIES *

François FAGES and Gérard HUET
CNRS (LITP), INRIA (Rocquencourt), 78153 Le Chesnay Cedex, France

Communicated by M. Nivat
Received October 1985

Abstract. We propose an abstract framework to present unification and matching problems. We argue about the necessity of a somewhat complicated definition of a basis of unifiers. In particular, we prove the nonexistence of complete sets of minimal unifiers (and matchers) in some equational theories, even regular.

1. Equational theories

We assume to be well known the concept of an algebra $A = \langle A, F \rangle$ with A a set of elements (the carrier of A) and F a family of operators given with their arities. More generally, we may consider heterogeneous algebras over some set of sorts, but all the notions considered here carry over to sorted algebras without difficulty and so we will forget sorts and even arities for simplicity of notation. With this provision, all our definitions are consistent with [22].

We denote by $T(F)$ the set of (ground) terms over F. We assume that there is at least one constant (operator of arity 0) in F so that this set is not empty. We also assume the existence of a denumerable set of variables V, disjoint from F, and denote by $T(F, V)$ the set of terms with variables over F and V. When F and V are clear from the context, we abbreviate $T(F, V)$ as T and $T(F)$ as G (for ground). We denote terms by $M, N, \ldots$, and write $V(M)$ for the set of variables appearing in M.

We denote by $\boldsymbol{T}$ (respectively $\boldsymbol{G}$) the algebra with carrier T(respectively G) and with operators the term constructors corresponding to each operator of F.

The *substitutions* are all mappings from V to T, extended to T, as endomorphisms of $\boldsymbol{T}$. We denote by S the set of all substitutions. If $\sigma \in S$ and $M \in T$, we denote by σM the application of σ to M. Since we are only interested in substitutions for their effect on terms, we shall generally assume that $\sigma x = x$, except on a finite set of variables $D(\sigma)$ which we call the *domain* of σ by abuse of notation. Such substitutions can then be represented by the finite set of pairs $\{x \leftarrow \sigma x \mid x \in D(\sigma)\}$.

* A preliminary version of this paper was presented in March 1983 at CAAP'83.

The empty substitution (identity) is denoted by Id. We define the set $I(\sigma)$ of *variables introduced by* σ as

$$I(\sigma) = \bigcup_{x \in D(\sigma)} V(\sigma x).$$

We say that σ is *ground* iff $I(\sigma) = \emptyset$. The composition of substitutions is the usual composition of mappings: $(\sigma \circ \rho)x = \sigma(\rho x)$. And we say that σ is *more general than* ρ: $\sigma \leqslant \rho$ iff $\exists \eta\ \eta \circ \sigma = \rho$, so Id is the smallest element (most general substitution).

An equation is a pair of terms $M = N$. Let E be a set of equations (axioms), we define the *equational theory presented by* E as the finest congruence over T containing all pairs $\sigma M = \sigma N$ for $M = N$ in E and σ in S. It is denoted by $=_E$. An equational theory presented by E is *axiomatic* iff E is finite or recursive.

An algebra A is a *model* of an equation $M = N$ if and only if $\nu M = \nu N$ as elements of A for every assignment ν (i.e., mapping from V to A extended as a morphism from T to A). We write $A \models M = N$. A is a model of an equational theory E iff $A \models e$ for every e in E. We denote by $\mathcal{M}(E)$ the class of models of E, which we call the *variety* defined by E.

E-equality in T is extended to substitutions by extensionality:

$$\sigma =_E \rho \quad \text{iff} \quad \forall x \in V\ \sigma x =_E \rho x.$$

We write, for any set of variables W,

$$\sigma =_E^W \rho \quad \text{iff} \quad \forall x \in W\ \sigma x =_E \rho x.$$

In the same way, σ is *more general than* ρ *in* E *over* W,

$$\sigma \leqslant_E^W \rho \quad \text{iff} \quad \exists \eta\ \eta \circ \sigma =_E^W \rho.$$

The corresponding equivalence relation on substitutions is denoted by $\equiv_E^W$; i.e., $\sigma \equiv_E^W \rho$ iff $\sigma \leqslant_E^W \rho$ and $\rho \leqslant_E^W \sigma$. We shall omit W when $W = V$ and E when $E = \emptyset$.

2. *E*-unification

2.1. Historical preliminaries

Let E be an equational theory. A substitution σ is an *E-unifier* of terms M and N if and only if $\sigma M =_E \sigma N$.

We denote by U_E the set of all E-unifiers of M and N:

$$U_E(M, N) = \{\sigma \in S \mid \sigma M =_E \sigma N\}.$$

The *unification problem* in E is the problem to decide whether, for any terms M and N, $U_E(M, N)$ is empty or not.

Hilbert's tenth problem (solving of polynomial equations over integers, called Diophantine equations) is the unification problem in arithmetic. Livesey, Siekmann, Szabo and Unvericht [33] have proved that associative-distributive unification is undecidable and thus, that the undecidability of Hilbert's tenth problem [7, 36] does not rely on a specific property of integers.

Axiomatic equational theories are semidecidable (e.g., by enumerating all possible proofs of equality of two terms), so U_E is always recursively enumerable (e.g., by enumerating all substitutions and checking in parallel whether they are unifiers or not), but, of course, we are mostly interested in a generating set of the E-unifiers (called 'Complete Set of E-Unifiers' in [39] and denoted by CSU_E), from which we can generate U_E by instantiations since $\sigma_M =_E \sigma N \Rightarrow \forall \eta\ (\eta \circ \sigma)M =_E (\eta \circ \sigma)N$. Or better, by a basis of U_E (called 'Complete Set of Minimal Unifiers' and denoted by $\mu\mathrm{CSU}_E$) satisfying the minimality conditions $\sigma \neq \sigma' \Rightarrow \sigma \not\leq_E^V \sigma'$, where $V = V(M) \cup V(N)$.

Hence, we shall make the difference between unification *procedures*, which enumerate a CSU_E (the exhaustive enumeration procedure in semidecidable theories enumerates U_E completely), unification *algorithms*, which always terminate with a finite CSU_E, empty if terms are not unifiable, and *minimal* unification procedures or algorithms which compute a $\mu\mathrm{CSU}_E$.

Unification was first studied in first-order languages (the case $E = \emptyset$) by Herbrand in [16]. In his thesis, he gave an explicit algorithm to compute a most general unifier. However, the notation of unification really grew out of the work of the researchers in automatic theorem-proving since the unification algorithm is the basic mechanism needed to explain the mutual interaction of inference rules. Robinson [41] gave the algorithm in connection with the resolution rule and proved that it indeed computes a most general unifier, that is, a $\mu\mathrm{CSU}_\emptyset$ equal to a singleton whose existence is a fundamental property of first-order languages. Independently, Guard [15] presented unification in various systems of logic. Unification is also central in the treatment of equality [29, 42]. Implementation and complexity analysis of unification is discussed in [1, 20, 25, 37, 50, 53] and Paterson and Wegman give a linear algorithm to compute a most general unifier.

First order unification was extended to infinite (regular) trees by Huet [20], who showed that a single most general unifier exists for this class, computable by an almost linear algorithm. This problem is relevant to the implementation of PROLOG-like programming languages [4, 5, 6, 9].

In the context of higher-order logic, the problem of unification was studied by Gould [14], who defined 'general matching sets' of terms, a weaker notion than that of CSU. The existence of unifier is shown to be undecidable in third-order languages in [18], and in second-order in [13]. The general theory of CSU's and μCSU's in the context of higher order logic is studied in [20, 24].

Unification in equational theories was first studied by Plotkin [39] in the context of resolution theorem provers to build up the underlying equational theory into the rules of inference. In this paper, Plotkin conjectured that there existed an equational theory E where a $\mu\mathrm{CSU}_E$ did not always exist. Theorem 2.1 in the next section proves this conjecture.

Further interest in unification in equational theories arose from the problem of implementing programming languages with 'call by patterns', such as QA4 [43]. Associative unification (finding solutions to word equations) is a particularly hard

problem. Plotkin [39] gives a procedure to enumerate a μCSU_A (possibly infinite), and Makanin [34] shows that the word equation problem is decidable. Stickel [47, 49] and, independently, Livesey and Siekmann [32, 33] give an algorithm for unification in the presence of associative-commutative operators, the termination of which has been proved in the general case by Fages [9, 10]. This result of termination has been generalized recently to the combination of unification algorithms for theories with disjoint sets of symbols by Kirchner [28], Tiden [51] and Yellick [52]. Siekmann [44] studied the general problem in his Ph.D. Thesis, especially the extension of the AC-unification algorithm to idempotence and identity. Lankford [30, 31] gave the extension to a unification procedure in Abelian group theory, for which Tiden [51] recently got a proof of termination.

The complexity of AC-unification is unknown. The complexity of AC-matching (i.e., finding one substitution σ such that $\sigma M =_{AC} N$) has been shown to be NP-complete by Chandra and Kannelakis (unpublished) and independently by Kapur et al. [26]. The complexity of AC-equivalence is linear.

In the class of equational theories for which there exists a canonical term rewriting system (see [22]), Fay [12] gives a universal procedure to enumerate a CSU_E. It is based on the notion of 'narrowing' as defined in [46]. Hullot [23] gives a similar procedure and a sufficient termination criterion, further generalized in [25]. Siekmann and Szabo [33] investigate the domain of regular canonical term rewriting systems in order to find general minimal unification procedures, but we shall show here that even in this framework μCSU_E may not exist (Theorem 4.2).

Termination or minimality of unification procedures is much harder to obtain than completeness. However, the main applications of unification in equational theories to the generalizations of the Knuth and Bendix algorithm, such as in [17, 38], are covered by the associative-commutative unification algorithm.

2.2. *Definitions*

Let $M, N \in T$, $V = V(M) \cup V(N)$, and W be a finite set of 'protected variables' not appearing in M or N, $W \cap V = \emptyset$. S is a *complete set of E-unifiers of M and N away from W* if and only if

(a) $\forall \sigma \in S\ D(\sigma) \subseteq V$ and $I(\sigma) \cap (W \cup D(\sigma)) = \emptyset$ (purity),

(b) $S \subseteq U_E(M, N)$ (correctness),

(c) $\forall \rho \subseteq U_E(M, N)\ \exists \sigma \subseteq S\ \sigma \leqslant_E^V \rho$ (completeness).

Furthermore, S is a *complete* set of *minimal* E-unifiers of M and N away from W if, additionally,

(d) $\forall \sigma, \sigma' \in S\ \sigma \neq \sigma' \Rightarrow \sigma \not\leqslant_E^V \sigma'$ (minimality).

The reason to consider W nonempty is that in equational theories in general some unifiers must introduce new variables and in many algorithms, unification is performed on subterms, so it is necessary to separate the variables introduced by unification from the variables of the context not appearing in M and N. This is the

case, for instance, for resolution in equational theories [39] and for the generalization of the Knuth–Bendix completion procedure in congruence classes of terms [38]. If W was not taken disjoint from V, then the variables in common should be renamed by the unifiers, e.g., with $W = V = \{x, y\}$, the substitution $\{x \leftarrow z, y \leftarrow z\}$ is a unifier of x and y which satisfies condition (a), but $\{x \leftarrow y\}$ or $\{y \leftarrow x\}$ are not. By taking $W \cap V = \emptyset$, variable renaming is not necessary. The condition $D(\sigma) \cap I(\sigma) = \emptyset$ is equivalent to *idempotence*: $\sigma \circ \sigma = \sigma$ and can always be satisfied by a unifier [8]; therefore, it is easy to show that there always exists a CSU_E away from W, by taking all E-unifiers satisfying (a).

However, we cannot put idempotence into the general definition of substitutions since, in order to compare two unifiers σ and ρ with the preorder $\leqslant$, we may have to consider a nonidempotent substitution ν. For example, with $\sigma = \{x \leftarrow f(y)\}$, $\rho = \{x \leftarrow f(f(y))\}$, and $V = \{x\}$, we have $\sigma \leqslant^V \rho$ by considering $\nu = \{y \leftarrow f(y)\}$. Moreover, the composition of idempotent substitutions is not necessarily idempotent.

Less strong than minimality we could add instead to the definition of CSU_E:

(d′) $\forall \sigma, \sigma' \in S\ \sigma \neq \sigma' \Rightarrow \sigma \not\equiv_E^V \sigma'$ (noncongruency).

Such CSU_E always exist but we lose the property that if U_E is recursively enumerable, then there exists a recursively enumerable one. For example, in undecidable axiomatic equational theories, U_E is recursively enumerable but in general the CSU_E satisfying (d′) are not.

2.3. *Existence of basis of E-unifiers*

It is well known that there may not exist a *finite* CSU_E. For instance, $a*x = x*a$ in the theory where $*$ is associative [39]. When there exists a finite CSU_E, there always exists a minimal one, by filtering out redundant elements. But it is not true in general, as is shown in the following theorem.

Theorem 2.1 (nonexistence of basis). *In some first-order equational theory E there exist E-unifiable terms for which there is no $\mu\mathrm{CSU}_E$.*

Proof. Let E be the equational theory defined by the function symbols 0, f, and g of arity 0, 2, and 1 and the two axioms

$$\begin{cases} f(0, x) = x, \\ g(f(x, y)) = g(y). \end{cases}$$

Let $M = g(x)$ and $N = g(0)$. We show that there does not exist a $\mu\mathrm{CSU}_E$ of M and N.

For the proof, we assume well-known the formalism of canonical term rewriting systems [22], i.e., simplification rules with finite and unique termination. It is easy to check that the system

$$R = \begin{cases} f(0, x) \to x, \\ g(f(x, y)) \to g(y) \end{cases}$$

is a canonical term rewriting system for E. We denote by $\to$ one step of reduction by R, as usual, by $\to^n$ a derivation of n reduction steps, and by $\downarrow[M]$ the normal form of term M in system R. We have $M =_E N$ iff $\downarrow[M] = \downarrow[N]$. The set of normal terms defines a model of E in the usual way. Let

$$\sigma_0 = \{x \leftarrow 0\}, \quad \sigma_1 = \{x \leftarrow f(x_1, 0)\},$$

$$\sigma_2 = \{x \leftarrow f(x_2, f(x_1, 0))\}, \ldots, \sigma_i = \{x \leftarrow f(x_i, \sigma_{i-1}x)\}, \ldots$$

and let $S = \{\sigma_i \mid i \geqslant 0\}$, $V = \{x\}$, $W = \emptyset$.

First we prove that S in a CSU_E of M and N away from W.

(1) Purity: $\forall i \geqslant 0\ D(\sigma_i) = \{x\}$ and $I(\sigma_i) \cap \{x\} = \emptyset$.

(2) Correctness: $\forall i \geqslant 0\ \sigma_i g(x) = g(f(x_i, f(x_{i-1}, \ldots, f(x_1, 0) \ldots))) \to^i g(0)$, so $\sigma_i M =_E N$.

(3) Completeness: Let $\sigma \in U_E(M, N)$ and $A = \downarrow[\sigma x]$, we have $g(A) =_E g(0)$. We show the completeness of S by proving $\exists i \geqslant 0\ \sigma_i x \leqslant A$ by structural induction on A.

- If A is a variable or a constant, then $g(A)$ is irreducible, so $g(A) =_E g(0)$ only if $A = 0$. We take $i = 0$.
- If $A = g(A')$, then $g(A) = g(g(A'))$ is also in R-normal form, so this case does not arise since the (unique) normal form is $g(0)$.
- If $A = f(A', A'')$, then $g(A) \to g(A'')$, so $g(A'') =_E g(0)$. By structural induction, we get a j such that $\sigma_j x \leqslant A''$, i.e., $\exists \rho \in S\ \rho\sigma_j x = A''$ with $D(\rho) \subseteq \{x_1, \ldots, x_j\}$. We take $i = j+1$, we have $\sigma_i x = f(x_i, \sigma_j x) \leqslant f(A', \sigma_j x)$ with substitution $\{x_i \leftarrow A'\}$, and we get $\sigma_i x \leqslant f(A', A'')$ with substitution $\rho \cup \{x_i \leftarrow A'\}$.

Now we show that for $i \geqslant 1$ $\sigma_i <_E^V \sigma_{i-1}$. For $i \geqslant 1$, let $\rho_i = \{x_1 \leftarrow 0\}$, we have

$$\rho_i \sigma_i x = f(0, \sigma_{i-1}x) \to \sigma_{i-1}x,$$

hence, $\sigma_i \leqslant_E^V \sigma_{i-1}$. Conversely, let us show that $\sigma_{i-1} \not\leqslant_E^V \sigma_i$ by contradiction. So let us assume that there exist some terms in R-normal form $A_{i-1}, \ldots, A_1$ such that $f(A_{i-1}, \ldots, f(A_1, 0) \ldots) =_E f(x_i, \ldots, f(x_1, 0) \ldots)$. The only normalization that may occur on the left member is the collapsing of the A_i's identical to 0, with the rule $f(0, x) \to x$, leading to a normal form $f(B_1, \ldots, f(B_k, 0) \ldots)$ with $k < i$, hence, distinct from the right member, leading to a contradiction. Now we can conclude the following.

Let R be any CSU_E of M and N. Since S is complete, we have $\forall \rho \in R\ \exists \sigma_i \in S\ \sigma_i \leqslant_E^V \rho$, and since $\sigma_{i+1} <_E^V \sigma_i$, we get $\sigma_{i+1} <_E^V \rho$. Since R is complete, we have $\exists \sigma \in R\ \sigma \leqslant_E^V \sigma_{i+1}$, therefore, we get $\sigma <_E^V \rho$: R is not minimal. □

However, when a $\mu\mathrm{CSU}_E$ exists, it is unique up to $\equiv_E^V$ [20].

Theorem 2.2 (unicity of basis). *Let M and N be two terms, U_1 and U_2 be two $\mu\mathrm{CSU}_E$ of M and N. There exists a bijection $\varphi : U_1 \to U_2$ such that $\forall \sigma \in U_1\ \sigma \equiv_E^V \varphi(\sigma)$.*

Proof. Since U_2 is complete, for any σ in U_1, there exists ρ in U_2 such that $\rho \leqslant_E^V \sigma$. We define $\varphi(\sigma)$ as one such substitution ρ. In the same way, since U_1 is complete,

$\forall \sigma' \in U_2\ \exists \rho' \in U_1\ \rho' \leqslant_E^V \sigma'$. We define $\psi(\sigma')$ as one such substitution ρ'. Therefore, $\forall \sigma \in U_1\ \psi(\varphi(\sigma)) \leqslant_E^V \varphi(\sigma) \leqslant_E^V \sigma$, so $\psi(\varphi(\sigma)) = \sigma$ by minimality. We get $\sigma \leqslant_E^V \varphi(\sigma) \leqslant_E^V \sigma$, that is, $\sigma \equiv_E^V \varphi(\sigma)$. □

3. *E*-matching

A substitution σ is a *E-matcher of M to N* iff $\sigma M =_E N$.

We remark that, when M and N have variables in common, matchers are not particular unifiers, for example, variable x is matchable to $f(x)$, although x and $f(x)$ are not unifiable. We define *complete sets of (minimal) E-matchers* of M to N away from W (denoted by CSM_E and $\mu\mathrm{CSM}_E$) in the same way as for unification, with the only difference that $V = V(M)$, W is a set of variables such that $W \cap V(N) = \emptyset$, and the purity condition becomes

$$\forall \sigma \in S\ D(\sigma) \subseteq V \text{ and } I(\sigma) \cap (W \setminus V(N)) = \emptyset.$$

When M and N do not share variables (which is the case in practice), we can take $V(M) \subseteq W$ which insures idempotence of matchers.

With the same proof as for Theorem 2.2 we can state that when a $\mu\mathrm{CSM}_E$ exists it is unique up to $\equiv_E^V$.

In the proof of Theorem 2.1, the example is in fact a matching problem since N is ground. Therefore, it shows also that there may not exist minimal complete set of E-matchers. One can notice that the situation is quite different from ω-order languages where minimal complete sets of matchers always exist [20] (and they are finite at order 2), although there may not exist a μCSU when the order is greater than 3.

4. Regular equational theories

We say that an equational theory E is *regular* iff for every axiom $L = R \in E$ we have $V(L) = V(R)$. This class of theories has been studied by several authors for their interesting properties in unification algorithms design [28, 45].

In regular theories variables cannot disappear. All the terms of a same class of congruence have the same set of variables, and so we may impose in our definition of matchers $V(M) \setminus V(N) \subseteq D(\sigma) \subseteq V(M)$ and $V(N) \setminus V(M) \subseteq I(\sigma) \subseteq V(N)$, and W is not necessary.

Even when N is ground, there may be no finite CSM_E of M to N (for example, $E = \{g(f(x, x)) = g(x)\}$, $M = g(x)$, $N = g(a)$), but the next proposition shows that there always exists a $\mu\mathrm{CSM}_E$ in this case, more precisely, in a regular theory E, any complete set of different E-matchers of a term M to a ground term N is minimal.

Proposition 4.1. *Let E be a regular theory, M and N be terms such that $V(N) = \emptyset$, Let $V = V(M)$ and S be a CSM_E of M to N. S is minimal iff $\forall \sigma, \sigma' \in S\ \sigma \neq \sigma' \Rightarrow \sigma \neq_E^V \sigma'$.*

Proof. For the nontrivial way, assume S is not minimal, i.e., $\exists \sigma, \sigma' \in S\ \sigma \neq \sigma'$ and $\exists \rho\ \rho\sigma =_E^V \sigma'$. Since E is regular and N is ground, we have $I(\sigma) = I(\sigma') = \emptyset$. Hence, $\forall x \in V\ V(\sigma x) = \emptyset$, so $\rho\sigma x = \sigma x$ and $\sigma x =_E^V \sigma' x$, leading to a contradiction. □

Again, however, a $\mu\mathrm{CSU}_E$ may not exist in a regular theory, for it may still be necessary to introduce new variables to express most general E-unifiers.

Theorem 4.2. *In some regular theory E, there exists E-unifiable terms for which there is no $\mu\mathrm{CSU}_E$.*

Proof. Let E be the equational theory defined by the function symbols 0, a, f, g of arity 0, 0, 2, 1, respectively, and R be the canonical term rewriting system:

$$R = \begin{cases} f(0, x) \to x, \\ f(x, 0) \to x, \\ g(f(x, y)) \to f(g(x), g(y)), \\ g(0) \to 0, \\ f(f(g(x), y), z) \to f(g(x), f(y, z)). \end{cases}$$

The proof of canonicity has been checked on the KB system [11], and is left here to the reader's computer. We denote by $\to$ one step of reduction by R, and by $\downarrow[M]$ the R-normal form of term M. First, we state a normal form lemma.

Lemma 4.3. *Let P and Q be two terms in R-normal form and different from 0. Then we have $\downarrow[f(P, Q)] = f(P_1, f(P_2, f(P_m, Q)\ldots))$ for some $m \geq 1$ and terms $P_1, \ldots, P_m$ in R-normal form. Moreover, $P = f(P_1, \ldots, f(P_{m-1}, P_m)\ldots)$.*

The proof by structural induction on P is omitted.

Proof of Theorem 4.2 (*continued*). Let $M = g(x)$ and $N = f(y, g(a))$, we shall show that there does not exist a $\mu\mathrm{CSU}_E$ of M and N. Let

$$\sigma_0 = \{x \leftarrow a, y \leftarrow 0\}, \qquad \sigma_1 = \{x \leftarrow f(x_1, a), y \leftarrow g(x_1)\},$$

$$\sigma_2 = \{x \leftarrow f(x_2, f(x_1, a)), y \leftarrow f(g(x_2), g(x_1))\}, \ldots,$$

$$\sigma_i = \{x \leftarrow f(x_i, \sigma_{i-1}x), y \leftarrow f(g(x_i), \sigma_{i-1}y)\}, \ldots$$

and $S = \{\sigma_i \mid i \geq 0\}$, $V = \{x, y\}$, $W = \emptyset$.

First we show that S is a CSU_E of M and N away from W.

(1) Purity: $\forall i \geq 0\ D(\sigma_i) = \{x, y\}$ and $I(\sigma_i) \cap \{x, y\} = \emptyset$.

(2) Correctness: $\forall i \geq 0\ \downarrow[\sigma_i M] = f(g(x_i), f(g(x_{i-1}), \ldots, f(g(x_1), g(a)) \cdots))$ by i applications of the third rule of R. In the same way we have $\downarrow[\sigma_0 N] = g(a)$ if $i = 0$, and if $i > 0$, we have $\downarrow[\sigma_i N] = \downarrow[\sigma_i f(y, g(a))] = \downarrow[\sigma_i g(x)]$ by $i - 1$ applications of the last rule of R, hence, $\sigma_i M =_E \sigma_i N$.

(3) Completeness: Let $\sigma \in U_E(M, N)$ and $A = \downarrow[\sigma x]$, $B = \downarrow[\sigma y]$, we have $g(A) =_E f(g(B), g(a))$. If $B \neq 0$, by Lemma 4.3, we have

$$\downarrow[\sigma N] = \downarrow[f(B, g(a))] = f(B_1, f(B_2, \ldots, f(B_m, g(a))\ldots))$$

and

$$B = f(B_1, f(B_2, \ldots, f(B_{m-1}, B_m)\ldots)) \quad \text{for some } m \geqslant 1.$$

We show the completeness of S by proving $\exists i \geqslant 0\ \sigma_i x \leqslant A$ and $\sigma_i y \leqslant B$ by structural induction on A.

Assume A is a variable or a constant. If $A \neq 0$, then $g(A)$ is in normal form, otherwise, $\downarrow[g(0)] = 0$. The only way to match with $\downarrow[\sigma N]$ is therefore $A = a$ and $B = 0$, and we take $i = 0$.

If $A = g(A')$, then $g(A) = g(g(A'))$ is also in R-normal form since there is no redex at top-level. $g(A)$ does not match any form of $\downarrow[\sigma N]$, so this case does not arise.

Assume $A = f(A', A'')$. $\downarrow[\sigma M] = \downarrow[g(f(A'), A'')] = \downarrow[f(g(A'), g(A''))]$. A' and A'' are different from 0 since A is in normal form, hence, by Lemma 4.3 on $P = \downarrow[g(A')]$ and $Q = \downarrow[g(A'')]$, we get

$$\downarrow[\sigma M] = f(A_1, f(A_2, \ldots, f(A_n, Q)\ldots))$$

and

$$P = f(A_1, f(A_2, \ldots, f(A_{n-1}, A_n)\ldots)) \quad \text{for some } n \geqslant 1.$$

For $\downarrow[\sigma M] = \downarrow[\sigma N]$, we have

- $m \geqslant n$,
- $\forall k \leqslant n\ A_k = B_k$,
- $Q = f(B_{n+1}, f(B_{n+2}, \ldots, f(B_m, g(a))\ldots))$ if $m \neq n$, and $Q = g(a)$ if $m = n$. Let

$$B'' = \begin{cases} 0 & \text{if } m = n, \\ B_m & \text{if } m = n-1, \\ f(B_{n+1}, f(B_{n+2}, \ldots, f(B_{m-1}, B_m)\ldots)) & \text{otherwise.} \end{cases}$$

By Lemma 4.3 we get $Q = \downarrow[f(B'', g(a))]$, hence, $\sigma'' = \{x \leftarrow A'', y \leftarrow B''\}$ is an E-unifier of M and N. By structural induction, $\exists j \geqslant 0\ \sigma_j \leqslant_E^V \sigma''$, i.e., $\exists \rho \in S\ \rho\sigma_j x =_E A''$ and $\rho\sigma_j y =_E B''$ with $D(\rho) \subseteq \{x_1, \ldots, x_j\}$. We take $i = j+1$, we get $\sigma_i x = f(x_i, \sigma_j x) \leqslant_E f(A', A'')$ and $\sigma_i y = f(x_i, \sigma_j y) \leqslant_E f(g(A'), B'')$ with substitution $\rho \cup \{x_i \leftarrow A'\}$.

Now we show that, for $i \geqslant 1$, $\sigma_i <_E^V \sigma_{i-1}$. For $i \geqslant 1$, let $\rho_i = \{x_i \leftarrow 0\}$, we then have $\rho_i\sigma_i x = f(0, \sigma_{i-1}x) \rightarrow \sigma_{i-1}x$, and $\rho_i\sigma_i y = f(g(0), \sigma_{i-1}y) \rightarrow^2 \sigma_{i-1}y$, hence, $\sigma_i \leqslant_E^V \sigma_{i-1}$. Conversely, let us show that $\sigma_{i-1} \not\leqslant_E^{\{x\}} \sigma_i$ by contradiction. So let us assume there exist some terms in R-normal form $X_{i-1}, \ldots, X_1$ such that

$$f(X_{i-1}, \ldots, f(X_1, a)\cdots) =_E f(x_i, \ldots, f(x_1, a)\cdots).$$

If a term X_j contains the symbol g, then the R-normal form of the left member still contains an occurrence of symbol g since the only rules of R that may apply preserve the number of occurrences of g, hence, we get a contradiction, for the right member does not contain any g. Otherwise, the only normalization that may occur on the left member is the collapsing of the X_i's identical to 0, with the rule $f(0, x) \rightarrow x$, leading to a normal form $f(Z_1, \ldots f(Z_k, a)\ldots)$ with $k < i$, hence, distinct from the right member, leading to a contradiction. Therefore, we can conclude the following.

Let R be any CSU_E of M and N. Since S is complete, we have $\forall \rho \in R\ \exists \sigma_i \in S\ \sigma_i \leqslant_E^V \rho$ and since $\sigma_{i+1} <_E^V \sigma_i$, we get $\sigma_{i+1} <_E^V \rho$. Since R is complete, we have $\exists \sigma \in R\ \sigma \leqslant_E^V \sigma_{i+1}$, therefore, we get $\sigma <_E^V \rho$: R is not minimal. □

We remark that the example in this proof is not a matching problem, so it does not subsume the example in the proof of Theorem 2.1 and does not prove our conjecture that there may also not exist a $\mu\mathrm{CSM}_E$ of M to N in a regular theory when N contains variables.

References

[1] L.D. Baxter, The complexity of unification, Ph.D. Thesis, Univ. of Waterloo, Ontario, 1977.

[2] L.D. Baxter, The undecidability of the third order dyadic unification problem, *Inform. and Control* **38** (1978) 170–178.

[3] R.M. Burstall, J.S. Collins and R.J. Popplestone, *Programming in* POP-2 (Edinburgh University Press, 1971).

[4] M. Van Caneghem, L'anatomie de Prolog II, Thèse de doctorat d'état, Univ. d'Aix-Marseille, 1984.

[5] A. Colmerauer, Prolog II, manuel de référence et modèle théorique, Rappt. Int., Groupe d'Intelligence Artificielle, Univ. d'Aix-Marseille II, 1982.

[6] A. Colmerauer, H. Kanoui and J. Van Caneghem, Étude et réalisation d'un système PROLOG, Rappt. Int., GIA, Univ. d'Aix-Marseille Luminy, 1972.

[7] M. Davis, Hilbert's tenth problem is unsolvable, *Amer. Math. Monthly* **80**(3) (1973) 233–269.

[8] E. Eder, Abstract properties of substitutions and unifiers, *J. Symbolic Comput.* **1** 1985.

[9] F. Fages, Formes canoniques dans les algèbres booléennes et application à la démonstration automatique en logique de premier ordre, Thèse, Univ. de Paris VI, 1983.

[10] F. Fages, Associative-commutative unification, Res. Rept. LITP, Paris; submitted to *J. Symbolic Comput.*; previous version as INRIA Rept. No. 287 presented at CADE'7, Lecture Notes in Computer Science **170** (Springer, Berlin, 1984).

[11] F. Fages et al., Le système KB: Présentation et bibliographie, mise en œuvre, Res. Rept. No. 368, INRIA France, 1985.

[12] M. Fay, First-order unification in an equational theory, *4th Workshop on Automated Deduction*, Austin, TX (1979) 161–167.

[13] W.D. Goldfarb, The undecidability of the second-order unification problem, *Theoret. Comput. Sci.* **13** (1981) 225–230.

[14] W.E. Gould, A matching procedure for omega order logic, Scient. Rept. 1, AFCRL 66-781, contract AF19 (628)-3250, 1966.

[15] J.R. Guard, Automated logic for semi-automated mathematics, Scient. Rept. 1, AFCRL 64-411, Contract AF19 (628)-3250, 1964.

[16] J. Herbrand, Recherches sur la théorie de la démonstration, Thèse, Univ. de Paris, 1930, in: *Écrits logiques de Jacques Herbrand* (PUF, Paris, 1968).

[17] J. Hsiang, Topics in automated theorem proving and program generation, Ph.D. Thesis, Univ. of Illinois at Urbana-Champaign, 1982.

[18] G. Huet, The undecidability of unification in third-order logic, *Inform. and Control* **22** (1973) 257–267.

[19] G. Huet, A unification algorithm for typed λ-calculus, *Theoret. Comput. Sci.* **1**(1) (1975) 27–57.

[20] G. Huet, Résolution d'équations dans des langages d'ordre 1, 2, ..., ω, Thèse d'État, Univ. de Paris VII, 1976.

[21] G. Huet, An algorithm to generate the basis of solutions to homogeneous, linear Diophantine equations, *Inform. Process. Lett.* **7**(3) (1978) 144–147.

[22] G. Huet and D. Oppen, Equations and rewrite rules: A survey, in: R.V. Book, ed., *Formal Languages: Perspectives and Open Problems* (Academic Press, New York/London, 1980).

[23] J.M. Hullot, Compilation de formes canoniques dans les théories équationnelles, Thèse de 3ème cycle, Univ. de Paris Sud, 1980.

[24] D. Jensen and T. Pietrzykowski, Mechanizing ω-order type theory through unification, *Theoret. Comput. Sci.* **3** (1977) 123-171.

[25] J.P. Jouannaud and C. Kirchner, Incremental construction of unification algorithms in equational theories, *Proc. 10th ICALP*, 1983.

[26] D. Kapur et al., Complexity of matching problem, *Proc. Rewrite Techniques and Applications*, Dijon, 1985, Lecture Notes in Computer Science **202** (Springer, Berlin, 1985) 417-429.

[27] H. Kirchner and C. Kirchner, Contribution à la résolution d'équations dans les algèbres libres et les variétés équationnelles d'algèbres, Thèse de 3ème cycle, Univ. de Nancy, 1982.

[28] C. Kirchner, Méthodes et outils de conception systématique d'algorithmes d'unification dans les théories équationnelles, Thèse d'état, Univ. de Nancy, 1985.

[29] D. Knuth and P. Bendix, Simple word problems in universal algebras, in: J. Leech, ed., *Computational Problems in Abstract Algebra* (Pergamon Press, Oxford/New York, 1970) 263-297.

[30] D.S. Lankford, A unfication algorithm for Abelian group theory, Rept. MTP-1, Math. Dept., Louisiana Techn. Univ., Ruston, LA, 1979.

[31] D.S. Lankford, G. Butler and B. Brady, Abelian group unification algorithms for elementary terms, Math. Dept., Louisiana Techn. Univ., Ruston LA, 1983.

[32] M. Livesey and J. Siekmann, Unification of bags and sets, Int. Rept. 3/76, Institut für Informatik I, Univ. Karlsruhe, 1976.

[33] M. Livesey, J. Siekmann, P. Szabo and E. Unvericht, Unification problems for combinations of associativity, commutativity, distributivity and idempotence axioms, *4th Workshop on Automated Deduction*, Austin, TX (1979) 161-167.

[34] G.S. Makanin, The problem of solvability of equations in a free semigroup, *Akad. Nauk. SSSR. TOM* **23**(2) (1977) 287-290.

[35] A. Martelli and U. Montanari, An efficient unification algorithm, *ACM TOPLAS.* **4**(2) (1982) 258-282.

[36] Y. Matiyasevich, Diophantine representation of recursively enumerable predicates, *Proc. 2nd Scandinavian Logic Symposium* (North-Holland, Amsterdam, 1970).

[37] M.S. Paterson and M.N. Wegman, Linear unification, *J. Comput. System Sci.* **16** (1978) 158-167.

[38] G.E. Peterson and M.E. Stickel, Complete sets of reduction for equational theories with complete unification algorithms, *J. ACM* **28**(2) (1981) 233-264.

[39] G. Plotkin, Building-in equational theories, *Machine Intelligence* **7** (1972) 73-90.

[40] P. Raulefs, J. Siekmann, P. Szabo and E. Unvericht, A short survey on the state of the art in matching and unification problems, *Sigsam Bull. 1979* **13** (1979).

[41] J.A. Robinson, A machine-oriented logic based on the resolution principle, *J. ACM* **12** (1965) 32-41.

[42] G.A. Robinson and L.T. Wos, Paramodulation and theorem proving in first-order theories with equality, *Machine Intelligence* **4** (1969) 135-150.

[43] J.F. Rulifson, J.A. Derksen and R.J. Waldinger, QA4: A procedural calculus for intuitive reasoning, Tech. Note 73, A.I. Center, SRI, Menlo Park, 1972.

[44] J. Siekmann, Unification and matching problems, Ph.D. Thesis, Memo CSM-4-78, Univ. of Essex, 1978.

[45] J. Siekmann and P. Szabo, Universal unification in regular equational ACFM theories, *6th CADE*, New York, 1982.

[46] J.R. Slagle, Automated theorem-proving for theories with simplifiers, commutativity and associativity, *J. ACM* **21** (1974) 622-642.

[47] M.E. Stickel, A complete unification algorithm for associative-commutative functions, *4th Internat. Joint Conf. on Artificial Intelligence*, Tbilisi, U.S.S.R., 1975.

[48] M.E. Stickel, Unification algorithms for artificial intelligence languages, Ph. D. Thesis, Carnegie-Mellon University, Pittsburgh, PA, 1976.

[49] M.E. Stickel, A complete unification algorithm for associative-commutative functions, *J. ACM* **28**(3) (1981) 423-434.

[50] M. Venturini Zilli, Complexity of the unification algorithm for first-order expressions, *Calcolo* **XII** (IV) (1975) 361-372.

[51] E. Tiden, Unification in combinations of theories with disjoint sets of function symbols, Royal Inst. of Technology, Dept. of Computer Science, S-100 44, Stockholm, 1985.
[52] K. Yellick, Combining unification algorithms for confined equational theories, M.I.T., Cambridge, MA, 1985.
[53] J.A. Robinson, Computational logic: The unification computation, in: B. Meltzer and D. Michie, eds., *Machine Intelligence Vol. 6* (American Elsevier, New York, 1971).